

HELEIN & MARASHLIAN, LLC 1483 Chain Bridge Road Suite 301 McLean, Virginia 22101 Telephone: (703) 714-1300 Facsimile: (703) 714-1330 E-mail: mail@CommLawGroup.com Website: www.CommLawGroup.com

Writer's Direct Dial Number 703-714-1313

Writer's E-mail Address jsm@commlawgroup.com

September 11, 2008

ELECTRONICALLY FILED

Marlene H. Dortch Secretary Federal Communications Commission 445 12th Street SW Washington, D.C. 20554

Re: Filed in EB Docket No. 06-36

Certification of CPNI Filing September 11, 2008

Dear Secretary Dortch:

On behalf of Business Automation Technologies, Inc. d/b/a Data Network Solutions, its attorneys hereby file its Certification of Compliance with Section 222 of the Communications Act and Commission Rules implementing Section 222.

An additional copy of this filing is also enclosed, to be date-stamped and returned in the envelope provided.

Should there be any questions regarding this filing, kindly contact the undersigned.

Respectfully submitted,

/s/

Jonathan S. Marashlian

Enclosure

CPNI CERTIFICATION

I, Isaac Fajerman, certify that I am an officer of the company named above and acting as an agent of the above-named company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. §64.2001 et seq.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission) against data brokers in the past year. The company has no information to report with respect to the processes pretexters are using to attempt to access CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized use of CPNI.

Isaac Fajerman President

Accompanying Statement of Annual CPNI Compliance Certification

Indicate below (X) whether the Company has taken any or all of the following actions to protect against the unlawful disclosure of CPNI.

Employee Training and Discipline

X Trained all employees and personnel as to when they are and are not authorized to use CPNI. X Instituted an express disciplinary process for unauthorized use of CPNI. Sales and Marketing Campaign Approval X Guaranteed that all sales and marketing campaigns are approved by management. **Record-Keeping Requirements** X Established a system to maintain a record of all sales and marketing campaigns that use their customers' CPNI, including marketing campaigns of affiliates and independent contractors. X Ensured that these records include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. X Made certain that these records are maintained for a minimum of one (1) year. **Establishment of a Supervisory Review Process** X Established a supervisory review process for all outbound marketing situations. X Certified that under this review process, all sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval. Opt-In Guaranteed that the Company only disclosed CPNI to agents, affiliates, joint venture partners, independent X contractors or to any other third parties only after receiving "opt-in" approval from a customer. Verified that the Company enters into confidential agreements with joint venture partners, independent contractors X

or any other third party when releasing CPNI.

Opt-Out Mechanism Failure

Established a protocol through which the Company will provide the FCC with written notice within five (5) business days of any instance where opt-out mechanisms do not work properly, to such a degree that customers' inability to opt-out of more than an anomaly.

Compliance Certificates

- Executed a statement, signed by an officer, certifying that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the FCC's CPNI regulations.
- X Executed a statement detailing how operating procedures ensure compliance with CPNI regulations.
- X Executed a summary of all customer complaints received in the past year concerning unauthorized release of CPNI.

Customer Authentication Methods

- Instituted customer authentication methods to ensure adequate protection of customers' CPNI. These protections only allow CPNI disclosure in accordance with the following methods:
 - X Disclosure of CPNI information in response to a customer providing a pre-established password;
 - X Disclose of requested CPNI to the customer's address or phone number of record; and
 - Access to CPNI if a customer presents a valid photo ID at the carrier's retail location.

Customer Notification of CPNI Changes

- Established a system under which a customer is notified of any change to CPNI. This system, at minimum, notifies a customer of CPNI access in the following circumstances:
 - --password modification;
 - --a response to a carrier-designed back-up means of authentication;
 - --online account changes; or
 - --address of record change or creation.

Notification of Law Enforcement and Customers of Unauthorized Access

X Established a protocol under which the appropriate Law Enforcement Agency ("LEA") is notified of any

Data Network Solutions

a division of Rusiness Automation Technologies Inc.

unauthorized	access to	o a cueto	mar's	CDNI
unaumorized	access i	o a cusic	imer s	UPNI

X Ensured that all records of any discovered CPNI breaches are kept for a minimum of two (2) years.